2.8 Applicant/Licensee Record

The following checklist summarizes the Licensing Procedures for NCES Restricted-Use Data.

Applicant/Licensee Record	
ACTIVITY	✓

REVIEW REQUIRED PROCEDURES	
Obtain a copy of the *Restricted-Use Data Procedures Manual.*	
Review the manual.	

APPLYING FOR A LICENSE (page 2-8)	
Submit the following documents to the NCES Data Security Officer.	
Formal Letter of Request (page 2-9) on organization letterhead:	
(1) Title of survey(s).	
(2) Description of the statistical research project for which the restricted-use data are needed. Explanation of why the restricted-use data are needed (e.g., instead of the public data version). Explanation of how the statistical research project is consistent with the specific purpose for which the survey was conducted.	
(3) Name and title of the Senior Official.	
(4) Name and title of the Principal Project Officer(s).	
(5) Names and titles of the professional/technical staff.	
(6) Estimated loan period (not to exceed five years).	
(7) Desired computer media format.	

Applicant/Licensee Record, continued

Activity	✓
APPLYING FOR A LICENSE, continued	
License Document (page 2-11)	
(1) Complete and sign the appropriate license document.	
Affidavit(s) of Nondisclosure (page 2-12)	
(1) Ensure personnel who will execute Affidavits read and understand the License and the NCES Security Procedures. (2) Fill out and notarize Affidavits of Nondisclosure for all project personnel, including support staff.	
Security Plan (page 2-13)	
(1) Write a Security Plan which addresses all applicable procedures identified in the NCES Security Procedures and any additional protections due to local conditions. It must be signed.	

NCES REVIEW

NCES will review the submitted documents for content and completeness.

If all requirements have been met, the requested materials will be sent to the new Licensee.

UNDER NO CIRCUMSTANCES may the data base be removed or communicated from the Licensee's site.

Applicant/Licensee Record, continued

Activity	✓
REQUIRED LICENSEE ACTIVITY (page 2-15)	
Maintaining the License File (page 2-15)	
Have on file at the licensed facility, copies of:	
(1) The **License Document** and its three attachments,	
(2) **Amendments** to the license document,	
(3) All executed **Affidavit(s) of Nondisclosure**, and	
(4) Licensee's submitted **Security Plan**.	
All project staff must know where these documents are kept.	
Submitting Research Publications to NCES (page 2-16)	
(1) Forward to NCES for review an advance (before public release) copy of each publication that might disclose individually identifiable information. [NCES will formally notify the licensee of acceptance of the publication (i.e., no security violations were found).]	
(2) A final copy of each publication containing information based on NCES restricted-use data must be forwarded to NCES.	
Passing On-Site Inspections (page 2-16, also chapter 4)	
(1) After conducting an on-site inspection, NCES will provide formal notification of any violations in the security procedures.	
(2) All identified security violations must be corrected.	
(3) Notify NCES in writing of the corrective security measures.	

Applicant/Licensee Record, continued

ACTIVITY	✓

AMENDING A LICENSE (page 2-17)	
Notify NCES in writing if there have been any changes to the conditions of the license.	
(1) NCES must be notified of new and/or departing project personnel.	
(2) New personnel must complete Affidavits of Nondisclosure; those of departing personnel must be destroyed or otherwise canceled.	
(3) Changes in project purpose or product require a contract amendment approved by NCES.	
(4) Changes in, or additions to, licensed data base(s) require a contract amendment approved by NCES.	

CLOSING-OUT THE LICENSE PERIOD (page 2-19)	
(1) Formally notify NCES when the data project is completed.	
(2) Return the original subject data to NCES.	
(3) Return any additional data materials and documentation to NCES (if applicable).	
(4) Double check that a final copy of each publication containing information based on restricted-use data has been sent to NCES.	
(5) Destroy all hard copy versions of the subject data and purge all traces of the subject data, including all copies and subsets, from any computer system used in analysis.	